

(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(51) Int. Cl. ⁶

G06F 9/06

G06F 11/20

(21) 출원번호

특 1994-019752

(22) 출원일자

1994년06월10일

(30) 우선권주장

93-291658 1993년11월22일 일본(JP)

(11) 등록번호

특 0132998

(24) 등록일자

1997년 12월 16일

(73) 특허권자

후지쓰 가부시끼가이사 세끼자와 다다시

일본국 가나가와Ken 가와사끼시 나가하라구 가미고다나까 1015반찌

(72) 발명자

아이모도 다케시

일본국 가나가와Ken 가와사끼시 나가하라구 가미고다나까 1015반찌 후지스 가부시끼가이사 내

(74) 대리인

문기상, 조기호

실사과 : 오른수 (책자공보 제5360호)

(54) 바이러스 진단기구의 작성시스템과 작성방법 및 바이러스 진단장치와 진단방법

요약

컴파일러로 원시프로그램을 컴퓨터로 실행 가능한 목적프로그램으로 번역할 때 컴파일러의 하나의 기능으로서 마린원 진단목적 생성부에 의해 목적프로그램내에 바이러스 진단부를 생성한다. 바이러스 진단부는 프로그램 사이즈의 검증, 검사법의 경증, 작성년월일 등의 개정정보의 검증, 디스크번지의 검증, 목적프로그램의 검증, 암축 및 복원을 이용한 목적프로그램의 검증등을 실시한다.

대표도**도1****영세서**

[발명의 명칭]

바이러스 진단기구의 작성시스템과 작성방법 및 바이러스 진단장치와 진단방법

[도면의 간단한 설명]

제1도는 본 발명에 사용되는 컴파일러의 블록도.

제2도는 본 발명에 의한 바이러스 진단기구의 생성을 나타낸 도면.

제3도는 컴파일러 기능의 블록도.

제4도는 본 발명에 의한 바이러스 진단기구의 제1실시예의 블록도.

제5도는 제4도에 나타낸 처리동작의 플로차트.

제6도는 바이러스 감염방지 처리의 플로차트.

제7A도, 제7B도는 바이러스 감염전과 감염후의 프로그램 구조를 나타낸 도면.

제8A도, 제8B도는 바이러스 감염이 판단되었을 경우에 형성된 프로그램 구조를 나타낸 도면.

제9도는 본 발명에 의한 바이러스 진단기구의 제2실시예의 블록도.

제10도는 제9도에 나타낸 처리동작의 플로차트.

제11도는 본 발명에 의한 바이러스 진단기구의 제3실시예의 블록도.

제12도는 제11도에 나타낸 처리동작의 플로차트.

제13도는 본 발명에 의한 바이러스 진단기구의 제4실시예의 블록도.

제14도는 제13도에 나타낸 처리동작의 플로차트.

제15도는 본 발명에 의한 바이러스 진단기구의 제5실시예의 블록도.

제16도는 제15도에 나타낸 바이러스 진단기구의 생성과 그 진단처리를 나타낸 도면.

제17도는 제15도에 나타낸 처리동작의 플로차트.

제18도는 본 발명에 의한 바이러스 진단기구의 제6실시예의 블록도.

제19도는 제18도에 나타낸 바이러스 진단기구의 생성과 그 진단처리를 나타낸 도면.

제20도는 제18도에 나타낸 처리동작의 플로차트.

[발명의 핵심한 설명]

본 발명은 컴퓨터 바이러스 감염을 예방하기 위한 바이러스 진단기구의 작성시스템과 작성방법 및 바이러스 진단장치와 진단방법에 관한 것이다. 특히 바이러스가 침입했을 때 함재로서 작용하는 바이러스 진단기구의 작성시스템과 작성방법 및 바이러스 진단장치와 진단방법에 관한 것이다.

근년에 개발된 컴퓨터 시스템에서는 컴퓨터 바이러스의 발생에 수반해서 바이러스 감염을 방지할 수 있는 기능이 요구되고 있다. 지금까지는 외부로부터 침입한 컴퓨터 바이러스의 감염에 의해 파일파괴 등의 이상이 생겼을 경우에는 컴퓨터 바이러스의 기능을 무효화시키는 컴퓨터 백신들을 개발하여 바이러스 감염을 방지하고자 하였다.

그러나 종래의 컴퓨터 백신을 사용한 바이러스의 감염방지에서는 신형의 바이러스가 발생하면 백신의 개발에 잠시간이 걸려서 개발 기간동안에 바이러스에 감염하는 우려가 있었다. 또한 바이러스에 감염하여도 파일이 하나 지워질 정도의 피해를 발견하는 일은 거의 없고, 바이러스 감염을 알아차릴 때 까지에 파일파괴들의 피해가 결정적으로 확대해버리는 문제가 있었다.

본 발명에 의하면 컴퓨터에 의한 목적 프로그램(object program)으로의 번역단계에서 바이러스 진단기구를 자동적으로 생성하고 OS(운영체제) 또는 프로그램으로서 실행되는 목적프로그램 자체로 바이러스 감염을 진단할 수 있도록 한 바이러스 진단기구의 작성방법과 작성장치 및 바이러스 진단장치와 진단방법을 제공한다.

진단목적 생성부에 의해 생성되는 바이러스 진단부는 다음 기능중의 어느 하나를 실현한다.

I. 프로그램 사이즈의 검증.

II. 검사함(checksum)의 검증.

III. 작성년월일등의 개정정보의 검증.

IV. 디스크번지의 검증.

V. 목적프로그램의 검증.

VI. 암축 및 복원을 이용한 목적 프로그램의 검증.

[프로그램 사이즈의 검증]

컴파일부에 의해 번역된 목적프로그램의 원사이즈를 기억시켜 둔다. 컴퓨터로 운영체제 또는 프로그램으로서 적재(load)되고 실행된 목적프로그램의 실행사이즈를 검출하여 원사이즈와 비교한다. 암자가 일치할 경우에는 처리를 속행하고, 일치하지 않을 경우에는 바이러스 감염으로 판단하여 처리를 중단한다.

[검사함의 검증]

컴파일부에 의해 번역된 원목적프로그램의 검사함을 기억시켜 둔다. 컴퓨터로 운영체제 또는 프로그램으로서 적재되고 실행된 목적프로그램의 검사함을 검출하여 원검사함과 비교한다. 암자가 일치할 경우에는 처리를 속행하고, 일치하지 않을 경우에는 바이러스 감염으로 판단하여 처리를 중단한다.

[개정정보의 검증]

컴파일부에 의해 번역된 원목적프로그램의 개정정보를 기억시켜 둔다. 컴퓨터로 운영체제 또는 프로그램으로서 적재되고 실행된 목적프로그램의 개정정보를 비교한다. 암자가 일치할 경우에는 처리를 속행하고, 일치하지 않을 경우에는 바이러스 감염으로 판단하여 처리를 중단한다.

개정정보로서는 갱신을 포함한 작성년월일, 갱신을 포함한 작성시각, 작성자명, 프로그램명, 버전 번호(version number)등의 적어도 하나를 사용한다.

[디스크번지의 검증]

컴파일부에 의해 번역된 원목적프로그램이 격납된 곳을 가리키는 디스크번지를 기억시켜 둔다. 컴퓨터로 운영체제 또는 프로그램으로서 적재되고 실행된 목적프로그램의 디스크번지를 검출하여 원디스크번지와 비교한다. 암자가 일치할 경우에는 처리를 속행하고, 일치하지 않을 경우에는 바이러스 감염으로 판단하여 처리를 중단한다.

[목적프로그램의 검증]

컴파일부에 의해 번역된 목적프로그램을 원프로그램으로서 그대로 기억시켜 둔다. 컴퓨터로 운영체제 또는 프로그램으로서 적재되고 실행된 목적프로그램과 비교한다. 암자가 일치할 경우에는 처리를 속행하고, 일치하지 않을 경우에는 바이러스 감염으로 판단하여 처리를 중단한다.

[암축 및 복원을 이용한 목적프로그램의 검증]

컴파일부에 의해 번역된 원목적프로그램을 암축하여 기억시켜 둔다. 컴퓨터로 운영체제 또는 프로그램으로서 적재되고 실행된 목적프로그램을 편집하고 동시에 암축목적프로그램을 신장(伸長)하여 복원시킨다. 그

리고 복원목적과 실행목적을 비교한다. 양자가 일치할 경우에는 처리를 속행하고 일치하지 않을 경우에는 바이러스 감염으로 판단하여 처리를 중단한다. 목적프로그램의 실행에 의한 프로그램의 재기팅(rewriting)을 방지하는 캔신급지부를 커파일단계에서 부기하도록 하여도 좋다.

또한 본 발명은 진단목적 생성부에 생성된 바이러스 진단기구, 즉 바이러스 진단목적 자체를 대상으로 한다.

본 발명에 의하면 커파일러를 사용하여 원시프로그램이 목적프로그램으로 번역되는 목적생성시에 목적생성시에서 밖에 알 수 없는 정보로서의 바이러스 진단기구를 생성하여 목적내에 매입하고 있다. 그러므로 컴퓨터의 운영체제 또는 프로그램으로서의 실행시에 바이러스에 의해 목적이 재기팅되었을 경우에 목적자체가 갖는 바이러스 진단기구에 의해 재기팅된 것을 목적이 인식할 수 있게 된다. 따라서 목적이 바이러스 감염되었다고 판단한 경우에는 실행을 중단하여 바이러스의 피해를 최소화할 수 있다.

본 발명의 상기 및 그밖의 목적, 특징 이점등에 대해서는 도면을 참조한 하기의 상세한 설명으로 자명해 질 것이다.

제1도는 본 발명에 의한 바이러스 진단기구를 매입한 목적 프로그램의 작성에 사용되는 커파일러 마신을 나타낸 것이다. 주기억장치(200)는 운영체제(OS)를 기억하여 전원부팅시에 커파일러를 실행하는 프로그램이 전개된다. 주기억장치(202)는 주기억장치(200)에 대응하도록 배치되어 있다. 주기억장치(202)에 CPU(204)와 채널 프로세서(208)가 장착되어 있다. CPU(204)는 주기억장치(200)에 있는 번역된 커파일러 프로그램에 따라 원시프로그램을 컴퓨터로 실행가능한 어셈블리어나 기계어로 표현된 목적프로그램으로 번역하는 커파일을 실행시킨다. 자기디스크 유닛들을 사용한 각 파일장치(220, 230, 250, 260)은 채널버스(210)를 통해서 채널 프로세서(206)의 채널장치(208)에 접속된다. 파일장치(220)는 커파일을 실시하는 원시프로그램을 기억한다.

파일장치(230)는 각 커파일 처리과정에서 생성되는 중간파일(240)을 기억한다. 파일장치(250)는 바이러스 진단기구를 갖는 커파일이 끝난 목적프로그램을 기억한다. 파일장치(260)는 커파일처리과정에서 기호표(symbol table)를 기억한다. 채널, 채널 프로세서(206)의 다른 채널장치에는 CRT, 프린터, 키보드등(도시하지 않음)의 다른 입력력기기와 접속된다.

제2도는 본 발명에 의한 바이러스 진단기구를 갖는 목적프로그램 생성순서를 개략적으로 나타낸 것이다. 원시프로그램(10)은 COBOL, FORTRAN등의 적당한 프로그래밍 언어를 사용하여 작성되어 파일장치에 파일명으로서 적재된다. 커파일부(12)는 원시프로그램(10)을 입력하여 대상이 되는 컴퓨터로 실행가능한 어성을 리어나이스 기계어로 표현된 목적프로그램으로 번역하고 파일정보로서 목적프로그램(16)을 출력한다. 본 발명에서는 진단목적생성부(14)와 커파일부(12)내에 새로운 모드인 마이도어 있다. 진단목적생성부(14)는 커파일부(12)에 의해 원시프로그램(10)의 목적프로그램(16)으로 번역될 때 이 목적프로그램(16)내에 바이러스 진단기구를 자동적으로 생성한다. 진단목적생성부(14)가 바이러스 진단기구(18)를 생성하는 기능은 원시프로그램(10)에 의존하지 않으므로 바이러스 진단기구(18)는 원시프로그램(10)의 내용 여하에 관계없이 원시프로그램(10)을 커파일부(12)를 통과시킴으로써 차지적으로 목적프로그램(16)내에 매입되게 된다.

따라서 원시프로그램(10)의 작성단계에서는 본 발명에 의한 바이러스 진단기구(18)를 전혀 의식할 필요가 없다.

제3도는 제2도의 진단 목적 생성부(14)를 갖춘 커파일부(12)의 구성과 기능을 나타낸 것이다. 이 커파일의 기능은 제1도의 CPU(204)의 프로그램을 실행할 때 실현된다. 커파일자는 어휘해석부(26), 구문해석부(30), 중간코드생성부(34), 코드최적화부(38), 원래생성부(44) 및 진단목적생성부(14)로 구성된다. 어휘해석부(26)는 원시프로그램(10)을 입력한다. 어휘해석부(26), 구문해석부(30), 중간코드생성부(34) 및 코드최적화부(38)는 각각 중간파일(28, 32, 36 및 42)을 생성한다. 어휘해석부(26)는 COBOL이나 FORTRAN등의 소정의 프로그램언어로 기입된 원시프로그램(10)을 입력하여 프로그램언어의 어휘를 해석한다. 즉, 어휘해석부(26)는 프로그램언어로 기입된 원시프로그램(10)을 토큰(token)이라고 불리우는 단위 마디로 분할하여 그 단위의 정당성을 체크한다. 어휘해석부(26)는 원시프로그램(10)의 모든 어휘의 정당성을 체크하고 나서 토큰의 집합으로 된 중간파일(28)을 출력하여 이 중간파일(28)을 구문해석부(30)으로 보낸다.

구문해석부(30)는 어휘해석부(26)에서 생성된 중간파일(28)을 입력하여 원시프로그램(10)이 재운영 프로그래밍언어의 문법규칙에 맞히는지의 여부를 체크한다. 원시프로그램(10)이 문법 규칙에 합치하고 있으므로 구문해석부(30)는 원시프로그램(10)을 실행하는 순서를 정하고 이를 중간파일(32)으로 출력한다.

이 구문해석부(30)에 의한 구문해석은 일반적으로 2개의 기능을 갖추고 있다. 2개중의 하나는 원시프로그램(10)상의 토큰의 문법적으로 올바른 있는지의 여부를 체크하는 것이다. 두번째 기능은 원시프로그램(10)상의 모든 토큰의 존재 의미를 해석하고 나서 모든 토큰의 실행순서를 정하고 그 순서를 토큰의 트리이나 그룹의 형태로 표현되는 것이다. 일반적으로 각 토큰의 실행순서의 분석결과는 파서트리(parser tree)로 표현된다.

중간코드생성부(34)는 구문해석부(30)에 의해 작성된 중간파일(36)의 파서트리를 입력하여 커파일러가 가지고 있는 고유의 중간코드로 번역하여 중간파일(36)을 출력한다. 대표적인 중간코드로서는 3 피연산자 방식(3-operand method)이 알려져 있다. 코드 최적화부(38)는 중간코드 생성부(34)에서 얻어진 중간파일(36)의 중간코드를 입력하여 목적 루프타겟(target computer) 상에서 가장 적은 음량으로 그리고 가장 빠른 속도로 실행 가능한 중간언어로 번역하여 중간파일(42)을 출력한다. 일반적인 최적화의 수법으로서는 로컬한 최적화와 루프의 최적화의 수법으로서는 로컬한 최적화와 루프의 최적화가 대표적이다. 로컬한 최적화는 어분의 명령을 줄이는 수법이고, 루프의 최적화는 루프를 매번 실행할 때마다 같은 값을 나타낸 표현이 있을 경우에는 이를 우조건 루프 밖으로 추방하여 최초의 루프만을 실행하도록 한 수법이다. 코드생성부(44)는 코드최적화가 끝난 중간코드 또는 중간언어를 입력하여 목적 컴퓨터의 명령세트로 번역한다.

또한 본 발명은 진단목적생성부(14)를 갖추어서 코드생성부(44)로부터 최종적인 번역결과로서 얻어진 목적컴퓨터의 명령세트내에 바이러스 진단기구(18)를 구성하는 명령세트를 가한다. 그러므로 진단목적 생성

부(14)에 의해 가해지는 바이러스 전단기구(18)는 육적컴퓨터의 영형 세트로 된 어셈블리어 또는 기계어로 기입된 상태로 준비되어 있다. 물론 원시프로그램에 사용한 프로그램명언어나 컴파일러내의 중간언어로 표현된 바이러스 전단기구는 준비하여 대응하는 펌파일과정의 단계에서 번역프로그램내에 매입하도록 하여도 좋다. 바이러스 전단기구(18)가 전단목적생성부(14)에 의한 육적프로그램내에 매입된 후에 육적프로그램(16)은 파일정보로서 출색된다. 이와같이 컴파일러로 원시프로그램(10)으로부터 번역된 바이러스 전단기구(18)를 매입한 육적프로그램(16)은 풀로피디스크, 자기테이프등의 매체 또는 온라인에 의해 대상 컴퓨터의 ROM이나 디스크 유닛에 프로그램 파일로서 제공되여진다.

제4도는 본 발명에 의해 원시프로그램내에 매입된 바이러스 전단기구(18)의 제1실시예를 나타낸 것이다. 바이러스 전단기구(18)는 프로그램, 사이즈, 검출부(22), 사이즈판단부(22) 및 원사이즈기억부(24)로 구성된다. 원사이즈기억부(24)에는 제2도, 제4도에 나타낸 바와같이 컴파일부(12)에 의해 육적프로그램(16)을 작성한 때의 프로그램 사이즈, 애플들이 바이트수가 전단목적 생성부(14)에 의한 바이러스 전단기구(18)의 생성시에 세트되어 있다. 프로그램사이즈 검출부(20)는 이 바이러스 전단기구(18)를 갖춘 원시프로그램이 컴퓨터의 상의 OS 또는 프로그램으로서 실행되는 상태에서 프로그램이 바이러스 전단기구(18)의 처리로 진행될 때의 기동 암력을 받아서 바이러스 전단기구(18)가 매입되어 있는 육적프로그램의 바이트 수를 검출한다. 사이즈 판단부(22)는 프로그램 사이즈 검출부(20)로부터 실행프로그램의 사이즈가 양이 지면 원사이즈 기억부(24)에 기록된 원사이즈와 비교한다. 실행프로그램 사이즈가 원사이즈와 일치하고 있으며 바이러스 암력에 의한 프로그램 파괴가 없으므로 사이즈 판단부(22)는 속행출력을 발생한다. 따라서 처리는 육적프로그램내의 바이러스 전단기구(18)의 매입과 일치한다고 판단하여 계속되는 다음 프로그램 처리로 복귀한다. 실행프로그램의 사이즈가 원사이즈와 일치하지 않을 경우에는 바이러스 감염에 의해 이상한 처리가 가해져서 육적프로그램의 프로그램 사이즈가 변화한 것임을 알 수 있다. 이러한 경우에는 바이러스 감염이 되었고 판단하여 중단출력을 발생시켜 이후의 육적프로그램 실행을 방지한다. 육적프로그램이 중단되면 바이러스 감염에 의한 처리중단의 예시지를 조작자 콘솔(operator console) 등에 출력한다.

제5도는 제4도에 나타낸 바이러스 전단기구(18)의 처리동작을 나타낸 것이다. 처리가 육적프로그램의 처리로부터 바이러스 전단기구의 처리로 이동되고 현재 실행하고 있는 자신의 육적프로그램 사이즈를 스텝S1에서 검출한다. 스텝S2에서 이전 기억되어 있는 원사이즈와 비교하여 일치 여부를 판단한다. 일치가 일치하지 않으면 진행은 다시 정상의 육적프로그램의 처리로 복귀한다. 검출한 프로그램 사이즈가 원사이즈와 일치하지 않으면 바이러스 감염에 의한 프로그램 사이즈의 변화라고 판단하여 스텝3에서 처리를 중단한다.

제6도 컴퓨터 바이러스의 감염방지 처리의 일례를 나타낸 것이다. 바이러스 감염방지 처리는 스텝S1에서 OS 또는 프로그램의 최후에 바이러스를 복사(copy)하고, 스텝 S2에서 OS 또는 프로그램으로부터 바이러스를 호출하기 위하여 파괴하는 명령을 자신의 최후에 복사하고, 다음에 스텝 S3에서 OS 또는 프로그램으로부터 바이러스를 호출하도록 수정형으로써 이루어진다.

제7A도는 감염되지 않은 육적프로그램(48)을 나타낸 것이다. 육적프로그램(48)은 처리를 50-1-50으로 누락된 처리1-1을 순차적으로 실행하는 구조를 가지고 있다. 상기와 같은 구조를 가지고 있는 육적프로그램(48)이 제1도에 나타낸 바이러스에 감염되어 제7B도에 나타난 감염후 원시프로그램(52)과 같이 프로그램 구조가 변화한다. 즉 바이러스 처리를 블록(54)이 처리리를 50-1의 처리 1에 이어서 바이러스가 자신을 복사한 본래의 원시프로그램(48)의 처리리를 블록(53)의 처리3으로 복귀한다. 이렇게 구성된 프로그램구조는 증가영역(60)이 바이러스 감염에 의해 본래의 원시프로그램에 가해지는 결과로 된다.

제8B도는 바이러스 감염전의 본 발명에 의해 원시프로그램(48)을 나타낸 것이다. 콤파일할 때 생성된 바이러스 전단기구(18)는 처리를 블록 50-3과 50-4로 나타난 처리2와 처리4사이에 매입된다. 상기 바이러스 전단기구(18)의 매입한 육적프로그램(48)의 사이즈는 애플들이 100k 바이트이며, 이것이 원사이즈로서 제4도에 나타난 원사이즈기억부(24)에 미리 세트되어 있다.

제8A도의 육적프로그램(48)이 바이러스에 감염되어 육적프로그램(48)은 제8B도에 나타난 바와같이 육적프로그램(56)으로 된다. 이 육적프로그램은 원 육적프로그램(48)의 최후에 바이러스 자신을 복사한 바이러스 처리를 블록(54)에 이전하여 구조를 갖는다. 또한 바이러스를 호출하기 위하여 파괴하는 명령으로서 처리리를 50-3의 처리2가 세트된다. 다음에 육적프로그램(48)의 처리리를 50-1의 처리1로 부터 바이러스를 복사한 바이러스 처리를 블록(54)에 이전하여 파괴되며 되는 처리리를 50-2의 처리2로 부터 다시 육적프로그램(48)의 처리리를 블록 50-3의 처리3으로 복귀하는 프로그램 구조를 만들어 낸다. 상기의 바이러스 감염이 처리를 50-2의 처리2로 일어나면 감염전 100k바이트였던 프로그램 사이즈가 감염에 의해 애플들이 10k 바이트의 증가영역(60)이 가해져서 110k바이트의 프로그램 사이즈로 변화해버린다. 이와같은 프로그램래미 사이즈의 변화에 대하여 본 실시예에서는 처리리를 50-3의 처리3에 이어서 제4도에 나타난 전단기구(18)가 구비되어 있으며, 제5도의 플로터를 따라서 바이러스 전단처리가 실행된다. 이 경우에는 프로그램 사이즈가 원사이즈 100k 바이트로부터 110k 바이트로 전환되어 육적프로그램의 처리를 중단할 수 있다. 그러므로 육적프로그램을 계속 실행함으로써 바이러스 감염이 더이상 파지는 것을 방지할 수 있다. 또 처리중단시 조작자 콘솔에 바이러스 감염에 의한 처리중단의 예시지 출력을 육적프로그램의 프로그램 명칭이나 번호와 일몰려 할 수 있기 때문에 특정한 프로그램이나 OS에 바이러스 감염이 생긴 것을 통지할 수가 있다.

제9도는 본 발명에 의해 바이러스 전단기구(18)의 제2실시예를 나타낸 것이다. 제2실시예에 의한 바이러스 전단기구(18)는 검사할 검출부(62), 검사할 판단부(64) 및 원검사할 기억부(66)로 구성된다. 컴파일리로부터 출력되는 원시프로그램의 검사함은 원시 프로그램을 기억하는 ROM들의 예모리장치에서 소정사이즈의 예모리 블록마다 얹고 있으므로 이 얹어진 검사함을 원검사함으로서 원검사함으로서 원검사함 기억부(66)에 기억해둔다. 바이러스 전단기구(8)를 매입한 원시프로그램의 실행에 의해 앞에 위치한 처리가 중요하여 기동입력을 받으면 검사함 검출부(62)는 예모리 블록마다 위치한 검사함을 검출한다. 검사함 판단부(64)는 검출한 검사함을 대응하는 블록의 원 검사함과 비교한다. 양자가 일치하면 속행 출력을 발생하고, 일치하지 않으면 바이러스 감염으로 판단하여 중단출력을 의해 처리를 중단한다.

제10도는 제9도의 검사함을 사용한 바이러스 진단의 동작을 나타낸 것이다. 스텝 S1에서 목적프로그램의 선두블록의 검사함을 검출한다. 스텝 S2에서 검출된 검사함이 원검사함과 같는지의 여부를 체크한다. 양자가 같으면 처리는 스텝 S3으로 진행하여 모든 블록이 종료되어 있으면 다음 블록을 체크한다. 이렇게 하여 스텝 S1의 검사함의 검출과 스텝 S2의 원검사함과의 비교를 모든 블록의 진단종료까지 되풀이한다. 모든 블록의 검사함이 원검사함과 일치하지 않으면 처리는 원목적프로그램 처리로 복귀한다. 블록중의 어디에선가 검사함이 원검사함과 일치하지 않으면 처리는 스텝 S5로 진행하여 바이러스 강영으로 판단하고 처리를 중단한다.

제11도는 본 발명에 의한 바이러스 진단기구(18)의 제3실시예를 나타낸 것이다. 본 실시예에서는 웹시프로그램의 개정 정보를 이용하고 있다. 제3실시예에 의한 바이러스 진단기구는 개정정보 검출부(68), 개정판단부(70) 및 원개정장정보기억부(72)로 구성된다.

일반적으로, 목적프로그램은 프로그램의 선두구역에 버전 업(version up)등의 상태를 나타낸 개정영역을 갖는다. 이 개정영역에 따른 작성년월일, 작성시각, 작성자명, 프로그램명, 버전번호등이 기억되어 있다. 목적프로그램은 디스크 유닛의 디스크에 채상의 파일로 취급되고 있기 때문에 디스크에 채상의 파일내에 있는 개정영역도 포함된다. 따라서 작성년월일(작성년월일은 신년월일을 포함)(74), 작성시각(생신시각을 포함)(76), 작성자명(78), 프로그램명(80) 및 버전번호(82)는 컴퓨터처리가 실행될 때 바이러스 진단기구(18)의 원개정정보기억부(72)에 원래개정정보로서 세트된다. 바이러스 진단기구(18)는 매일 목적프로그램의 앞단계의 처리가 끝나자 기동입력을 받으면 개정정보를 검출부(60)에 의해 웹시프로그램의 개정영역으로부터 현재의 개정정보를 검출하여 개정판단부(70)로 보낸다. 개정판단부(70)는 검출된 개정정보와 원기저장정보기억부(72)에 기록된 정보를 비교한다. 양자가 일치하면 개정판단부(70)는 속행출력을 발생하고 일치하지 않으면, 바이러스 강영으로 판단하여 중단출력을 발생한다. 개정정보의 비교는 개정판단부(70)에서 실시되어 작성년월일(작성년월일을 포함)(74), 작성시각(생신시각을 포함)(76), 작성자명(78), 프로그램명(80), 버전번호(82)등이 모두 비교된다. 비교한 요소중의 어느 하나라도 일치하지 않으면 바이러스 강영으로 판단하여 중단출력을 발생한다. 바이러스 진단에 사용하는 개정정보는 작성년월일, 작성시각, 작성자명, 프로그램명 및 버전번호 중의 어느 것이나 하나이어도 좋다. 또한 이를 이외의 개정정보도 마찬가지로 취급한다.

제12도는 제11도의 바이러스 진단동작을 나타낸 것이다. 스텝 S1에서 목적프로그램의 개정영역의 정보를 검출한다. 스텝 S2에서 검출된 개정정보와 미리 세트된 원개정정보와 일치하는지의 여부를 판단한다.

양자가 일치하면 처리는 복귀하여 목적프로그램을 속행하고, 일치하지 않으면 바이러스 강영으로 판단하여 스텝 S3에서 처리를 중단한다.

제13도는 본 발명에 의한 바이러스 진단기구(18)의 제4실시예를 나타낸 것이다. 이 실시에는 디스크 번지를 사용하도록 한 것을 특징으로 한다. 본 제3실시예에 의한 바이러스 진단기구(18)는 디스크번지검출부(84), 디스크번지비교부(86) 및 웨이크스번지기억부(88)로 구성된다. 컴퓨터리더에 의해 작성된 목적프로그램은 목적컴퓨터 시스템의 입출력 서버 시스템을 구축하는 디스크 유닛에 기억된다. 그러므로 목적프로그램에는 기억부분을 가리키는 디스크 번지로서 예를들어 블록번호, 파일번호 및 트랙번지가 기입되어 있다. 컴퓨터리더에 의해 목적프로그램으로 바이러스 진단기구(18)를 생성하여 매일화 원디스크번지기억부(88)에 웨이크로그램의 기억부분이 되는 디스크번지를 가리키는 블록번호(90), 파일번호(92), 트랙번지(94)등을 기억해 둔다. 이 경우의 번지는 개시번지, 종료번지 또는 목적프로그램의 일련의 번지중의 어느 것이라도 좋다. 이 바이러스 진단기구(18)는 매일한 목적프로그램의 실행으로 바이러스 진단기구(18)가 기동입력을 받으면 디스크번지검출부(84)는 목적프로그램에 원 시점에서 기입되어 있는 디스크번지, 예를들어 블록번호, 파일번호 및 트랙번지를 검출하여 디스크번지 비교부(86)로 보낸다. 디스크번지비교부(86)는 웨이크스번지기억부(88)로 부터의 원정보로 블록번호(90), 파일번호(92) 및 트랙번지(94)를 판독하여 디스크번지기억부(88)로 부터의 원정보와 원정보가 일치하면 디스크번지 비교부(86)는 바이러스 강영되어 있지 않은 것으로 판단하여 속행 출력을 발생하여 목적프로그램을 계속 실행한다. 검출정보와 원정보가 일치하지 않으면 디스크번지 비교부(86)는 바이러스 강영으로 디스크번지의 부분이 파괴된 것으로 판단하여 중단출력을 발생한다.

제14도는 제15도에 나타난 바이러스 진동동작을 나타낸 것이다. 스텝 S1에서 디스크번지를 검출하여 스텝 S2에서 검출된 디스크번지가 원시자와 일치하는지의 여부를 판단한다. 양자가 일치하면 처리는 정상처리로 복귀한다. 양자가 일치하지 않으면 바이러스 강영으로 판단하여 스텝 S3에서 처리를 중단한다.

제15도는 본 발명에 의한 바이러스 진단기구(18)의 제5실시예이다. 이 제5실시예는 목적프로그램 전체를 원프로그램과 비교하여 바이러스 강영을 판독하도록 한 것을 특징으로 한다. 제5실시예에 의한 바이러스 진단기구(18)는 실행목적판독부(96), 목적비교부(98) 및 원목적기억부(100)로 구성된다. 원목적기기억부(100)은 원목적프로그램을 그대로 기억하고 있다.

제16도는 제15도에 나타난 제5실시예의 바이러스 진단동작을 나타낸 것이다. 컴퓨터리더에 배치된 진단목적 성생부(14)는 목적파일(220)이 받는 1회째의 출력으로 바이러스 진단기구(18)를 매일한 목적프로그램(16)을 기억한다. 이어서 목적프로그램(14)의 기능에 의해 바이러스 진단기구(18)를 매입하고 있지 않은 목적프로그램(102)을 2회째로 출력하여 목적파일(220)에 기억시킨다. 1회째에 출력한 바이러스 진단기구(18)를 매일한 목적프로그램(14)은 목적프로그램(102)을 목적파일(220)에 기억시킨다. 목적파일(220)에 초기 프로그램제작(IPL : initial-program-loaded)되어 OS 또는 프로그램으로서 실행된다. 이 OS 또는 프로그램으로서의 바이러스 진단기구(18)는 목적프로그램의 실행에서 바이러스 진단기구(18)는 제15도에 나타난 처리를 실시한다. 따라서 원목적기기억부(100)의 기능에 의해 목적파일(220)에 2회째로 출력되어 기억되어 있는 목적프로그램(102)이 원정보로서 판독되어 진단에 사용된다.

제17도는 제15도에 나타난 제5실시예의 바이러스 진단동작을 나타낸 것이다. 스텝 S1에서 에모리의 작업영역(working region)에 현재 실행되고 있는 목적프로그램을 판독하여 전개한다. 스텝 S2에서 외부의 파일장치(220)에 기억되어 있는 컴퓨터 시스템(104)에서 사용하고 있지 않는 원목적프로그램(102)을 미간자리로 작업영역에 판독하고 전개하여 스텝 S3에서 판독하여 실행하고 있는 목적프로그램과의 비교를 영령단위로 실시한다. 영령단위의 비교에서의 변수는 각 처리마다 다르므로 비교대상에서 제외한다. 영령

단위의 비교에서 원목적프로그램과 혼전히 일치하면 바이러스에 감염되어 있지 않은 것으로 판단하여 목적프로그램의 처리로 복귀한다. 명령단위의 비교에서 목적프로그램이 원목적프로그램과 일치하지 않으면 바이러스 감염으로 판단하여 스텝 S30로 처리를 중단한다. 제5실시시에의 바이러스 진단기구(18)는 제16도에 나타낸 바와 같이 목적프로그램의 사이즈를 기준으로 하는 프로그램 전체의 비교판단이 되기 때문에 진단처리에 시간이 걸린다. 그러므로 바이러스 진단기구(18)의 기동은 컴퓨터 시스템(104)의 유저루틴(idle routine)을 경출하여 유저시간에 실시하는 것이 바람직하다. 물론 사이즈가 작은 목적프로그램이면 목적프로그램의 각 실행마다 실시하여도 좋다.

제18도는 본 범위에 의한 바이러스 진단기구(18)의 제6실시시 예를 나타낸 것이다. 본 제6실시시에는 목적프로그램 전체의 비교판단을 실시함과 동시에 비교판단에 사용하는 원목적프로그램을 암축형식으로 출력하여 비교판단시에 신장하여 원목적프로그램으로 복원부록 하는 것을 특징으로 한다. 바이러스 진단기구(18)는 실행형식의 판독부(106), 목적파일교부(108), 암축목적기억부(110) 및 신장부(복원부)(114)로 구성된다. 암축목적기억부(110)에는 암축된 목적프로그램(112)이 기억되어 있다.

제19도는 제18도에 나타낸 제6실시시에의 바이러스 진단기구(18)의 생성상태를 나타낸 것이다. 컴퓨터일러(12)에 배치된 진단목적 생성부(14)는 1회째의 출력으로 제19도의 바이러스 진단기구(18)를 매입한 목적프로그램(16)을 목적파일장치(20)에 기억시킨다. 2회째의 출력으로 진단목적 생성부(14)는 바이러스 진단기구(18)를 매입하고 있지 않는 목적프로그램을 출력한다. 본 실시시에서는 진단목적 생성부(14)에 암축 알고리즘이 포함되어 있어서 목적프로그램을 암축한 후에 출력하여 목적파일장치(20)에 목적프로그램(112)으로서 기록시킨다. 진단목적 생성부(14)에 포함되는 암축 알고리즘으로써는 예를들어 2진 산술부호 알고리즘이 사용되어 목적프로그램(16)의 사이즈를 원사이즈의 2%정도까지 압축할 수가 있다. 따라서 암축목적프로그램(112)의 기억역을 대폭적으로 저감할 수 있다.

목적파일장치(20)에 기억되고 바이러스 진단기구(18)가 매입된 목적프로그램(16)은 목적컴퓨터 시스템(104)에 초기 프로그램 적재(190)되어 OS 또는 프로그램으로서 실행된다. 이 컴퓨터 시스템(104)에서의 목적프로그램(16)의 실행에서는 바이러스 진단기구(18)가 기동하면 목적파일장치(20)에 기억되어 있는 암축목적프로그램을 판독한다. 다음에 신장부(114)에서 암축목적프로그램(112)을 신장한 후에 목적파일교부(108)에서 현재 실행하고 있는 목적 프로그램과 비교하여 판단을 한다. 암축목적프로그램(112)을 신장하는 신장부(114)는 바이러스 진단기구(18)의 전용이 아니고 컴퓨터 시스템(104)이 가지고 있는 신장프로그램을 이용하는 것이 바람직하다.

제20도는 제18도에 나타낸 바이러스 진단동작을 나타낸 것이다. 스텝 S1에서 암축목적프로그램을 판독하고 스텝 S2에서 암축목적 프로그램을 신장하여 본 목적프로그램으로 전제를 비교해서 판단하므로 바이러스 진단처리에 시간이 걸린다. 그러므로 컴퓨터 시스템(104)의 유저시간에서 진단처리를 실시하는 것이 바람직하다. 물론 프로그램 사이즈가 적으면 목적프로그램 내에서 바이러스 진단처리를 실시하면된다.

본 범위의 다른 실시시에서 상술한 제1실시시~제6실시시 예의 어느 하나에 의한 바이러스 진단기구(18)에 대하여 목적프로그램(15)을 출력할 때 목적프로그램(16)에 간신금지 속성을 세트시키는 것이 바람직하다. 즉 목적프로그램(16)이 바이러스에 감염되면 목적프로그램은 제78도, 제88도에 나타난 바와같이 재기일된다. 그러므로 이와같은 바이러스 감염에 의한 재기일을 금지하여 위해 컴퓨터일러로 부터 목적프로그램에 출력을 때 간신금지 속성을 세트한다. 상술한 간신금지 속성의 세트는 목적프로그램(16)에 바이러스 감염이 있는 것으로 판단되고 처리는 목적프로그램의 처리로 복귀한다. 2개의 목적프로그램이 명령단위로 일치하지 않으면 바이러스 감염으로 판단되어 스텝 S5로 진행하여 처리를 중단한다.

제6실시시에서도 프로그램 사이즈가 경우에는 목적프로그램 전체를 비교해서 판단하므로 바이러스 진단처리에 시간이 걸린다. 그러므로 컴퓨터 시스템(104)의 유저시간에서 진단처리를 실시하는 것이 바람직하다.

본 범위의 다른 실시시에서 상술한 제1실시시~제6실시시 예의 어느 하나에 의한 바이러스 진단기구(18)에 대하여 목적프로그램(15)을 출력할 때 목적프로그램(16)에 간신금지 속성을 세트시키는 것이 바람직하다. 즉 목적프로그램(16)이 바이러스에 감염되면 목적프로그램은 제78도, 제88도에 나타난 바와같이 재기일된다. 그러므로 이와같은 바이러스 감염에 의한 재기일을 금지하여 위해 컴퓨터일러로 부터 목적프로그램에 출력을 때 간신금지 속성을 세트한다. 상술한 간신금지 속성의 세트는 목적프로그램(16)에 바이러스 감염이 있는 것으로 판단되고 처리는 목적프로그램의 처리로 복귀한다. 2개의 목적프로그램이 명령단위로 일치하지 않으면 바이러스 감염으로 판단되어 스텝 S5로 진행하여 처리를 중단한다.

상술한 바와같이 본 범위에 의하여 바이러스의 감염이 목적프로그램에 매입된 바이러스 진단기구에 의해 판단되어 처리를 중단되어 바이러스 감염에 의해 피해를 최소화로 억제하고 격퇴하고 격퇴한 바이러스 감염 방지력을 취할 수가 있다. 바이러스 진단기구는 컴퓨터일러에 마련된 진단목적 생성기능에 의해 컴퓨터일러 단계에서 목적프로그램에 자동으로 매입된다. 따라서 원시프로그램의 제조단계에서 바이러스 진단기구에 의식할 필요가 없으므로 원시프로그램의 제조행정이 자동화되어 실시된다. 또한 모든 원시프로그램의 컴퓨터일러 단계에서 목적프로그램내에 바이러스 진단기구가 자동적으로 매입되므로 목적 컴퓨터의 OS나 프로그램이 바이러스에 감염된 것을 조기에 발견하여 피해를 최소화한다.

본 범위의 바람직한 태양을 일부 대표적인 것으로 설명하지만 여기에 청구한 범위의 범위를 벗어나지 않는 한 상기 개시한 태양의 구조나 각부의 조합 및 배치를 변경할 수 있음은 물론이다.

(57) 청구의 범위

청구항 1

원시프로그램을 컴퓨터로 실행가능한 목적프로그램으로 번역하는 컴퓨터일러와, 상기 컴퓨터일러에 마련되어 상기 목적프로그램내에 미리 목적형식의 프로그램으로서 준비된 바이러스 진단부를 상기 목적프로그램의 진단에 적합한 내용으로 변경하여 조합한 진단목적 생성부를 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성시스템.

첨구항 2

제 1 항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 평파일러로 번역된 상기 목적프로그램의 원사이즈를 검출하여 기준 정보로서 기억한 원사이즈 기억부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 사이즈를 검출하는 실행사이즈 검출부와, 상기 원사이즈와 상기 실행사이즈를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않으면 경우에는 처리를 중단하는 사이즈 판단부를 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성시스템.

첨구항 3

제 1 항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 평파일러로 번역된 상기 목적프로그램의 원검사함을 검출하여 기준 정보로서 기억한 원검사함 기억부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 검사함을 검출하는 검사함 검출부와, 상기 원검사함과 상기 실행검사함을 비교하여 상기 두검사함이 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않으면 경우에는 처리를 중단하는 검사함 판단부를 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성시스템.

첨구항 4

제 1 항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 평파일러로 번역된 상기 목적프로그램의 원 개정정보를 검출하여 기준 정보로서 기억한 원개정정보기억부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 개정정보를 검출하는 개정정보검출부와, 상기 원 개정정보와 상기 실행 개정정보를 비교하여 상기 두 개정정보가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않으면 경우에는 처리를 중단하는 개정판단부를 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성시스템.

첨구항 5

제 1 항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 평파일러로 번역된 상기 목적프로그램의 원 개정정보를 검출하여 기준 정보로서 기억한 원개정정보기억부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 개정정보를 검출하는 개정정보검출부와, 상기 원 개정정보와 상기 실행 개정정보를 비교하여 상기 두 개정정보가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않으면 경우에는 처리를 중단하는 개정판단부를 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성시스템.

첨구항 6

제 1 항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 평파일러로 번역된 상기 목적프로그램의 기억저장소를 가리키는 디스크 범위를 검출하여 기준 정보로서 기억한 디스크번지기억부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 디스크번지 범위를 검출하는 디스크번지검출부와, 상기 원디스크번지와 상기 디스크번지와 상기 실행디스크번지 비교하여 두디스크번지가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않으면 처리를 중단하는 디스크번지 비교부를 갖춘 바이러스 진단기구의 작성시스템.

첨구항 7

제 1 항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 평파일러로 번역된 상기 목적프로그램을 원목적프로그램으로 하여 기준 정보로서 그대로 기억한 원목적 기억부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램을 비교대상으로서 만족하는 실행목적 만족부와, 상기 원목적 기억부의 암축목적 프로그램을 신장하여 비교대상으로 되돌리는 폭원부와, 상기 폭원목적과 상기 실행목적을 비교하여 상기 두 목적이 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않으면 처리를 중단하는 목적비교부를 갖춘 바이러스 진단기구의 작성시스템.

첨구항 8

제 1 항에 있어서,

상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 평파일러로 번역된 상기 목적프로그램의 원목적프로그램을 암축하여 기준 정보로서 기억한 암축목적 기억부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램을 비교대상으로서 만족하는 실행목적 만족부와, 상기 원목적 기억부의 암축목적 프로그램을 신장하여 비교대상으로 되돌리는 폭원부와, 상기 폭원목적과 상기 실행목적을 비교하여 상기 두 목적이 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않으면 처리를 중단하는 목적비교부를 갖춘 것으로 하는 바이러스 진단기구의 작성시스템.

첨구항 9

제2항-제7항중의 어느 1항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단부는 상기 목적프로그램의 실행에 의한 상기 프로그램 자신의 제기임을 금지하는 간신금지부를 더 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성시스템.

첨구항 10

원시프로그램을 컴퓨터로 실행가능한 목적프로그램으로 번역하는 평파일과정과, 상기 평파일 과정에서 상기 목적프로그램 내에 미리 목적형식의 프로그램으로서 준비된 바이러스 진단절차를 상기 목적프로그램의 진단에 적합한 내용으로 변형하여 조합하는 진단목적 생성과정을 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성방법.

첨구항 11

제10항에 있어서, 상기 진단목적 생성과정에서 생성된 상기 바이러스 진단절차는 상기 컴퓨터 과정에서 번역된 상기 목적프로그램의 원시코드를 검출하여 기준정보로서 기억하는 원시코드 기억과정과, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램을 검출하는 실행사이즈 검출과정과, 상기 원시코드와 상기 실행사이즈를 비교하여 상기 원시코드와 상기 실행사이즈가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않을 경우에는 처리를 중단하는 사이즈 판단과정을 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성방법.

청구항 12

제10항에 있어서, 상기 진단목적 생성과정에서 생성된 바이러스 진단절차는 상기 컴퓨터 과정에서 번역된 상기 목적프로그램의 원점코드를 기준정보로서 검출하여 기억한 원점코드 기억과정과, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 원점코드를 검출하는 실행사이즈 검출과정과, 상기 원점코드와 상기 실행사이즈를 비교하여 상기 원점코드와 상기 실행사이즈가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않을 경우에는 처리를 중단하는 사이즈 판단과정을 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성방법.

청구항 13

제10항에 있어서, 상기 진단목적 생성과정에서 생성된 바이러스 진단절차는 상기 컴퓨터 과정에서 번역된 상기 목적프로그램의 원개정정보를 기준정보로서 검출하여 기억하는 원개정정보기억과, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 원개정정보를 검출하는 개정정보 검출과정과, 상기 원개정정보와 상기 실행개정 정보를 비교하여 상기 두개정보가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않을 경우에는 처리를 중단하는 개정판단과정을 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성방법.

청구항 14

제13항에 있어서, 상기 개정정보로서 갱신을 포함한 작성년월일, 갱신을 포함한 작성시각, 작성자명, 프로그램명, 버전번호중의 적어도 하나를 사용하는 것을 특징으로 하는 바이러스 진단기구의 작성방법.

청구항 15

제10항에 있어서, 상기 진단목적 생성과정에서 생성된 바이러스 진단절차는 상기 컴퓨터 과정에서 번역된 상기 목적프로그램의 기억장을 가리키는 디스크 번지를 기준정보로서 검출하여 기억한 디스크 번지 기억과정과, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램의 디스크번지를 검출하는 디스크번지 검출과정과, 상기 원디스크번지와 상기 실행디스크 번지를 비교하여 상기 두디스크가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고 일치하지 않을 경우에는 처리를 중단하는 디스크 번지비교과정을 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성방법.

청구항 16

제10항에 있어서, 상기 진단목적 생성부에 의해 생성된 상기 바이러스 진단절차는 상기 컴퓨터로 번역된 상기 목적프로그램을 원목적프로그램을 기준정보로서 그대로 기억한 원목적 기억과정과, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램을 만들하는 실행목적판독과정과, 상기 원목적과 상기 실행목적을 비교하여 상기 두 목적이 일치할 경우에는 처리를 속행하고 일치하지 않으면 처리를 중단하는 목적비교과정을 갖춘 바이러스 진단기구의 작성방법.

청구항 17

제10항에 있어서, 상기 진단목적 생성과정에서 생성된 상기 바이러스 진단절차는 상기 컴퓨터 과정에서 번역된 상기 목적프로그램의 원목적 프로그램을 암축하여 기준정보로서 기억하는 암축목적기억과정과 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때, 상기 목적프로그램을 만들하는 실행목적판독과정과, 상기 원목적과 상기 실행목적을 비교하여 상기 두 목적이 일치할 경우에는 처리를 속행하고 일치하지 않으면 처리를 중단하는 목적비교과정을 갖춘 바이러스 진단기구의 작성방법.

청구항 18

제11항~제17항중의 어느 1항에 있어서, 상기 진단목적 생성과정에서 생성된 상기 바이러스 진단절차는 상기 목적프로그램의 실행에 의한 상기 프로그램의 제기입을 금지하는 갱신금지 과정을 더 갖춘 것을 특징으로 하는 바이러스 진단기구의 작성방법.

청구항 19

컴파일러에 의하여 컴퓨터로 실행가능한 형식으로 번역되어 컴퓨터에 적재된 운용체제 또는 프로그램으로서 실행되는 바이러스진단부를 갖춘 바이러스 진단장치에 있어서, 상기 목적프로그램으로부터 바이러스진단부에 사용하는 기준정보를 생성하여 기억하는 기준정보검출부와, 상기 컴퓨터의 운용체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램으로부터 예정된 바이러스진단부에 사용하는 실행정보를 검출하는 실행정보검출부와, 상기 기준정보와 상기 실행정보를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 판단부를 갖춘 것을 특징으로 하는 바이러스 진단장치.

청구항 20

제19항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 목적프로그램의 원사이즈를 기준정보로서 검출하여 기억하는 원사이즈 기억부이며, 상기 실행정보검출부는 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램의 사이즈를 검출하는 실행사이즈검출부이며, 상기 판단부는 상기 원사이즈와 상기 실행시의 사이즈를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 사이즈판단부인 것을 특징으로 하는 바이러스 진단장치.

청구항 21

제19항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 상기 목적프로그램의 원검사함을 기준정보로서 검출하여 기억하는 원검사함 기억부이며, 상기 실행정보검출부는 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램의 개정정보를 검출하는 개정정보검출부이며, 상기 판단부는 상기 원검사함과 상기 실행시의 개정정보를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 검사합판단부인 것을 특징으로 하는 바이러스 진단장치.

청구항 22

제19항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 상기 목적프로그램의 원개정정보를 기준정보로서 검출하여 기억하는 원개정정보기억부이며, 상기 실행정보검출부는 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램의 개정정보를 검출하는 개정정보검출부이며, 상기 판단부는 상기 원개정정보와 상기 실행시의 개정정보를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 개정판단부인 것을 특징으로 하는 바이러스 진단장치.

청구항 23

제22항에 있어서, 상기 개정정보로서 간신을 포함한 작성년월일, 간신을 포함한 작성시각, 작성자명, 프로그램명, 버전번호증의 적어도 하나를 사용하는 것을 특징으로 하는 바이러스 진단장치.

청구항 24

제19항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 상기 목적프로그램의 기억장소를 가리키는 디스크번지를 기준정보로서 검출하여 기억하는 디스크번지 기억부이며, 상기 실행정보검출부는 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램을 기준정보로서 검출하는 디스크번지기준정보로서 검출하는 디스크번지검출부이며, 상기 판단부는 상기 원디스크번지와 상기 실행시의 번지를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 디스크번지비교부인 것을 특징으로 하는 바이러스 진단장치.

청구항 25

제19항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 상기 목적프로그램을 기준정보로서 그대로 기억하는 원목적기억부이며, 상기 실행정보검출부는 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램을 비교대상으로 하는 디스크번지판독부이며, 상기 판단부는 상기 원목적기억부의 일속목적프로그램을 신장하여 본래대로 되돌리는 복원부와, 상기 원목적프로그램과 상기 실행목적프로그램을 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 목적비교부인 것을 특징으로 하는 바이러스 진단장치.

청구항 26

제19항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 상기 목적프로그램을 암축하여 기준정보로서 기억하는 암축목적기억부이며, 상기 실행정보검출부는 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램을 비교대상으로 하는 디스크번지판독부이며, 상기 판단부는 상기 원목적기억부의 일속목적프로그램을 신장하여 본래대로 되돌리는 복원부와, 상기 원목적프로그램과 상기 실행목적프로그램을 비교하여 양자가 일치된 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 목적비교부인 것을 특징으로 하는 바이러스 진단장치.

청구항 27

제20~제26항증의 어느 1항에 있어서, 상기 목적프로그램의 실행에 의한 프로그램 자체의 간신을 금지하는 간신금지부를 더 갖춘 것을 특징으로 하는 바이러스 진단장치.

청구항 28

컴퓨터리에 의하여 컴퓨터로 실행가능한 형식으로 번역되어 컴퓨터에 적재된 문운체제 또는 프로그램으로서 실행되는 목적프로그램의 바이러스진단방법에 있어서, 상기 목적프로그램으로부터 바이러스진단에 사용하는 기준정보를 생성하여 기억하는 기준정보검출과정과, 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램으로부터 애정된 바이러스진단에 사용하는 실행정보를 검출하는 실행정보검출과정과, 상기 기준정보와 상기 실행정보를 비교하여 양자가 일치된 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 면단과정들을 갖춘 것을 특징으로 하는 바이러스 진단방법.

첨구항 29

제28항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 목적프로그램의 원사이즈를 검출하여 기준정보로서 기억하는 원사이즈 기억과정이며, 상기 실행정보검출부는 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체의 처리루틴으로 들어갔을 때 상기 목적프로그램의 사이즈를 검출하는 실행사이즈검출과정이며, 이 판단과정은 상기 원사이즈와 상기 실행시의 사이즈를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 사이즈판단과정인 것을 특징으로 하는 바이러스 진단방법.

첨구항 30

제28항에 있어서, 상기 기준정보검출부는 상기 컴퓨터에서 번역된 상기 목적프로그램의 원점사함을 기준정보로서 검출하여 기억하는 원점사함 기억과정이며, 상기 실행정보검출과정은 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램의 실행시의 검사함을 검출하는 검사함검출과정이며, 상기 판단과정은 상기 원점사함과 상기 실행시 검사함을 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 검사함판단과정인 것을 특징으로 하는 바이러스 진단방법.

첨구항 31

제28항에 있어서, 상기 기준정보검출부는 상기 컴퓨터 과정에서 번역된 상기 목적프로그램의 원개정정보를 기준정보로서 검출하여 기억하는 원개정정보기억과정이며, 상기 실행정보검출과정은 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램의 개정정보를 검출하는 개정정보검출과정이며, 상기 판단과정은 상기 원개정정보와 상기 실행시의 개정정보를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 개정판단과정인 것을 특징으로 하는 바이러스 진단방법.

첨구항 32

제31항에 있어서, 상기 개정정보로서 견신을 포함한 작성년월일, 견신을 포함한 작성시각, 작성자명, 프로그램명, 버전번호증의 적어도 하나를 사용하는 것을 특징으로 하는 바이러스 진단방법.

첨구항 33

제28항에 있어서, 상기 기준정보검출과정은 상기 컴퓨터 과정에서 번역된 상기 목적프로그램의 기억장을 가리키는 디스크번지 기준정보로서 기억하는 디스크번지 기억과정이며, 상기 실행정보검출과정은 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램을 비교하여 양자가 일치할 경우에는 상기 원디스크번지와 상기 실행시의 번지를 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 디스크번지비교과정인 것을 특징으로 하는 바이러스 진단방법.

첨구항 34

제28항에 있어서, 상기 기준정보검출과정은 상기 컴퓨터 과정에서 번역된 상기 목적프로그램을 원목적 기준정보로서 그대로 기억하는 원목적기억과정이며, 상기 실행정보검출과정은 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램을 비교대상으로서의 편집하는 실행목적편집과정이며, 상기 판단과정은 상기 원목적프로그래그램과 상기 실행시의 목적프로그램을 비교하여 양자가 일치할 경우에는 상기 목적프로그램과 상기 목적비교과정인 것을 특징으로 하는 바이러스 진단방법.

첨구항 35

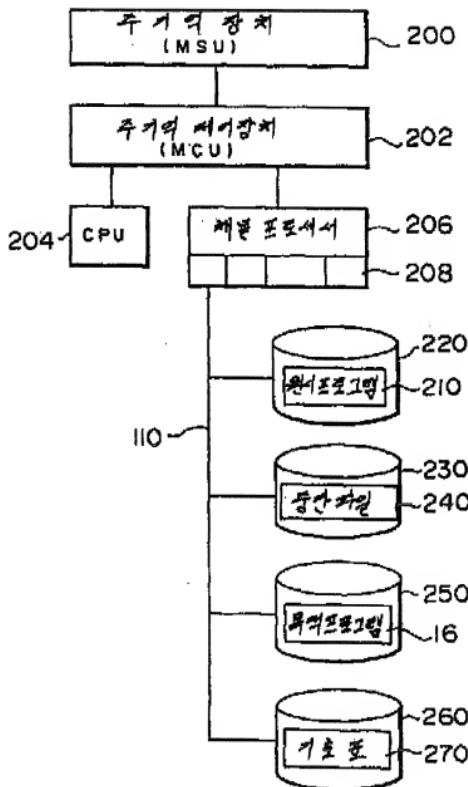
제28항에 있어서, 상기 기준정보검출과정은 상기 컴퓨터 과정에서 번역된 상기 목적프로그램을 암축하여 기준정보로서 기억하는 암축목적기억과정이며, 상기 실행정보과정은 상기 컴퓨터의 운영체제 또는 프로그램으로서 적재된 상기 목적프로그램의 실행중에 자체 처리루틴으로 들어갔을 때 상기 목적프로그램을 비교대상으로서 편집하는 실행목적편집과정이며, 상기 판단과정은 상기 암축목적기억과정의 암축목적프로그래그램을 신장하여 본래대로 되돌리는 복원과정과, 상기 복원목적과 상기 실행목적을 비교하여 양자가 일치할 경우에는 상기 목적프로그램의 처리를 속행하고, 일치하지 않을 경우에는 처리를 중단하는 목적비교과정인 것을 특징으로 하는 바이러스 진단방법.

첨구항 36

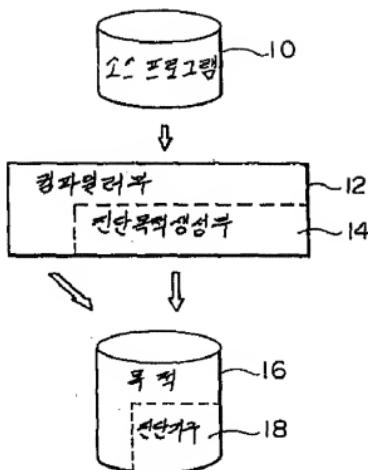
제28-35항중 어느 1항에 있어서, 상기 목적프로그램의 실행에 의한 프로그램 자체의 견신을 금지하는 견신금지과정을 더 갖춘 것을 특징으로 하는 바이러스 진단방법.

도연

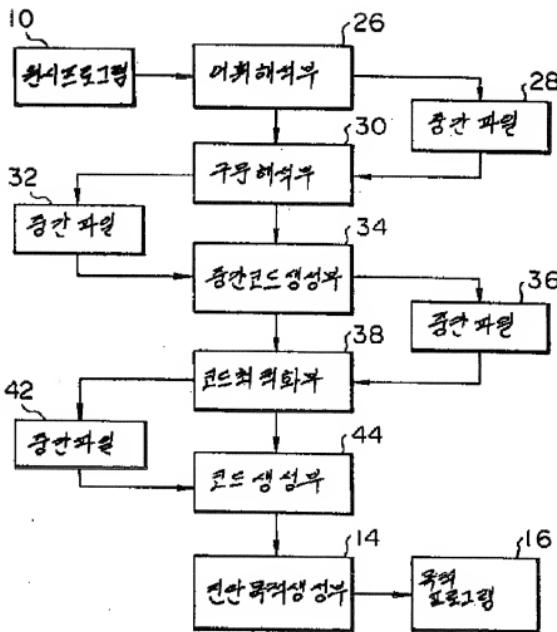
도면 1



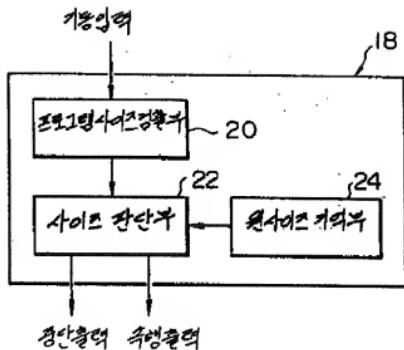
도면2



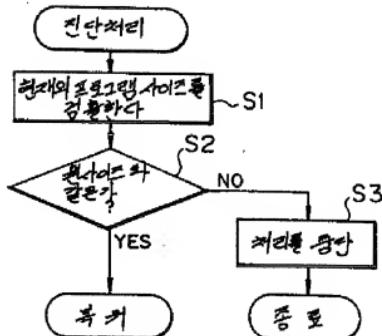
도면3



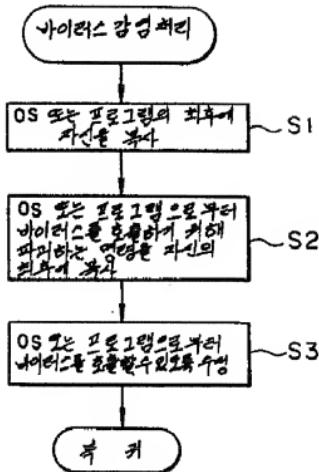
도면4



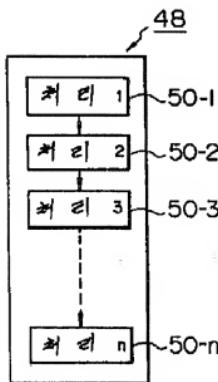
도면5



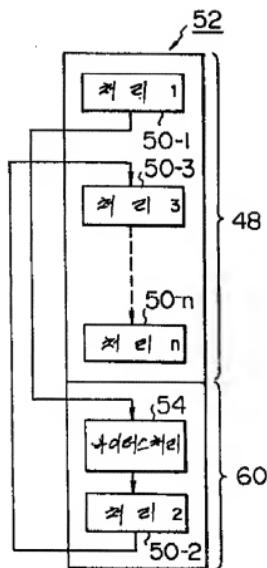
도면6



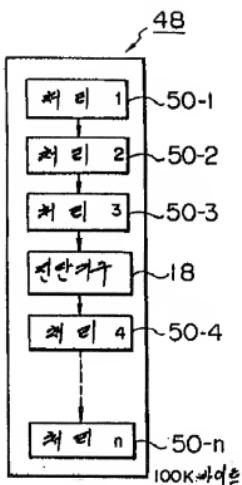
도면7a



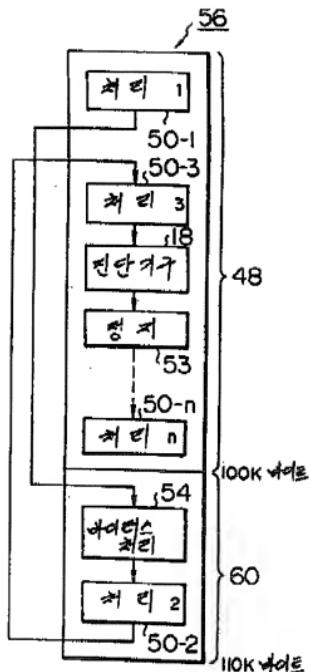
도면7b



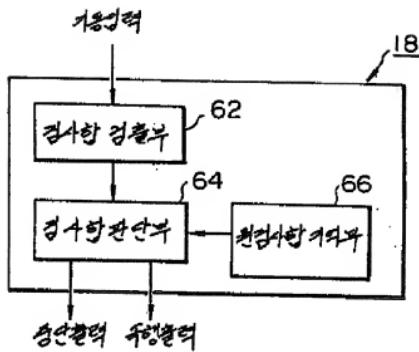
도면8a



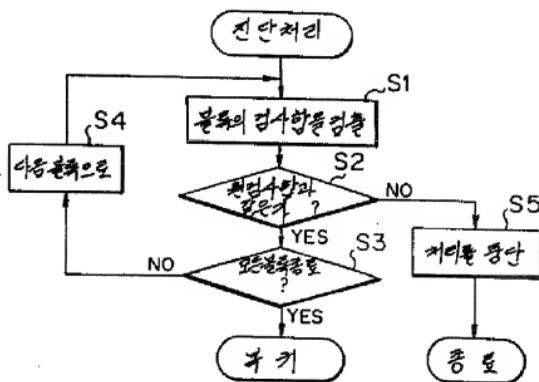
도면 6b



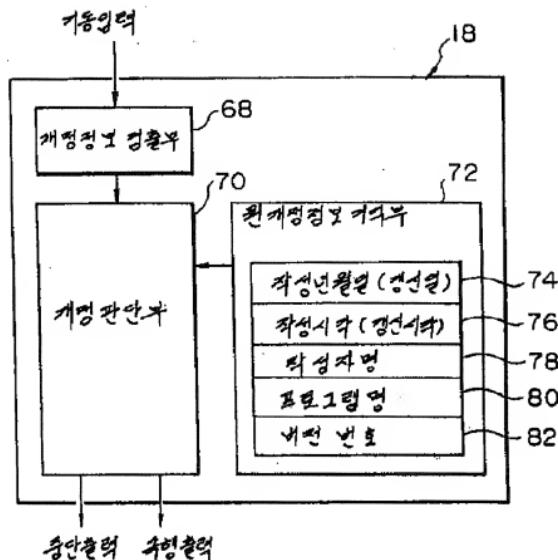
도면9



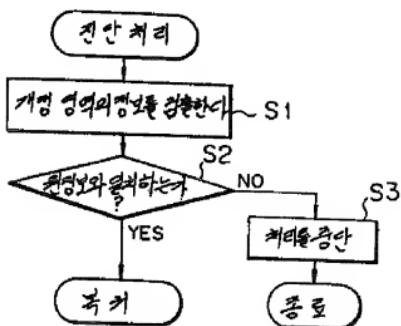
도면10



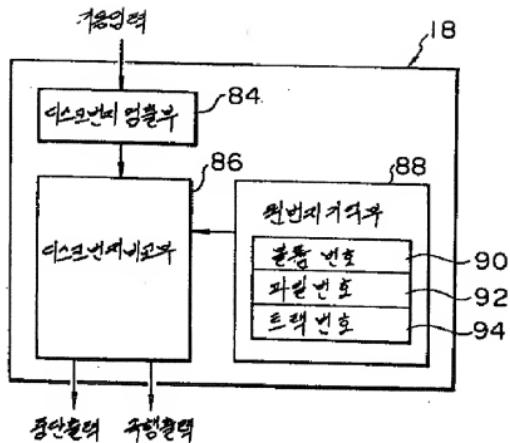
도면11



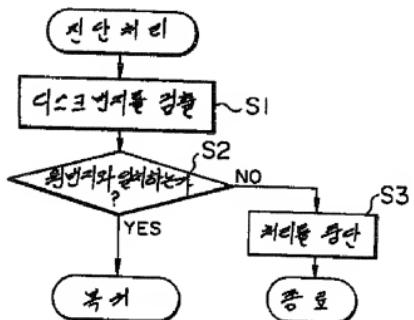
도면12



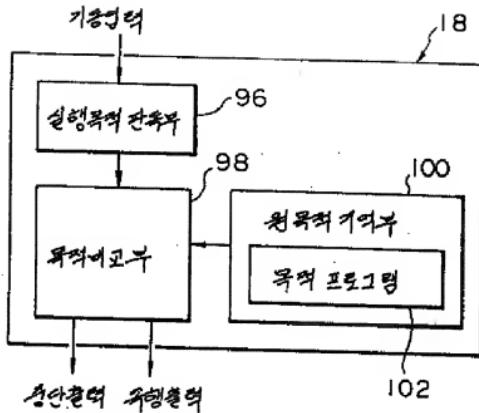
도면13



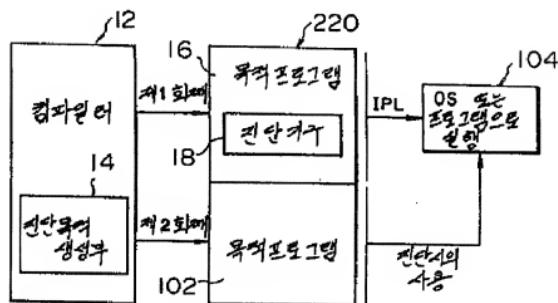
도면14



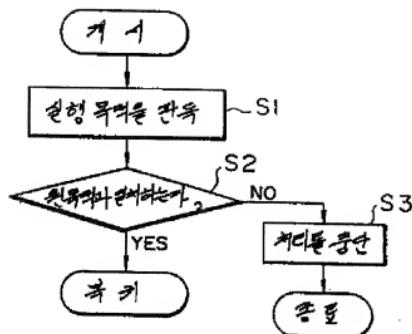
도면15



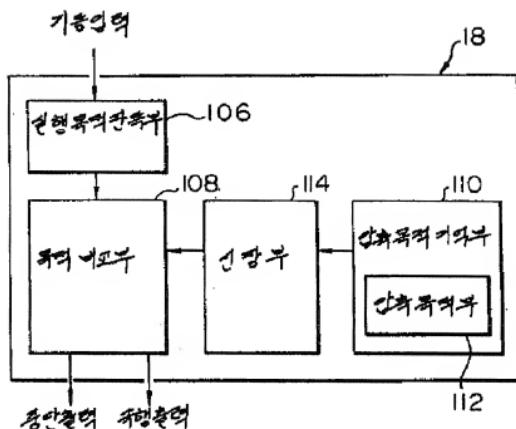
도면16



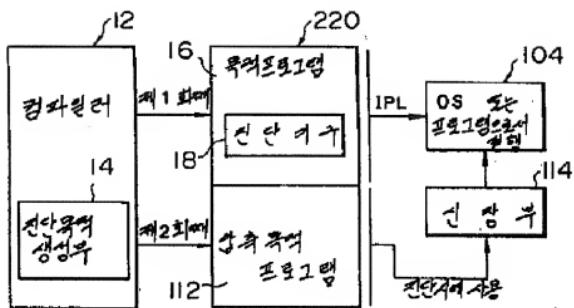
도면17



도면18



도면19



도면20

